Department of Administration

State Information Technology Services Division

RISK ASSESSMENT FOR ALERTING AND MONITORING

OF THE

STATEWIDE MICROWAVE NETWORK

In partnership with:

Document Owner: **State of Montana**

Previous Documents: **NONE**
Related Documents: **None**

Distribution: **State of Montana, Interoperability Montana, and Lewis & Clark County**

Issue & Amendment Record

Version	Date	Revised By	Comments
Draft 0.1	2/7/2011	J. Noland	State of Montana furnishes this technical risk assessment.

Table of Contents

INTRODUCTION

Risk assessment is the first process in risk management methodology. Organizations use risk assessment to determine the extent of a potential threat and the risk associated with an IT system throughout its life cycle. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, as discussed in Section 4.

Risk is a function of the ***likelihood*** of a given ***threat-source's*** ability to exercise a potential ***vulnerability***, and the resulting ***impact*** of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to the Statewide Microwave System must be analyzed in conjunction with potential vulnerabilities and controls in place for the system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. Risk assessment methodology encompasses nine primary steps, which are described in Sections 1 through 9 of this document.

- Step 1 - System Characterization (Section 1)
- Step 2 - Threat Identification (Section 2)
- Step 3 - Vulnerability Identification (Section 3)
- Step 4 - Control Analysis (Section 4)
- Step 5 - Likelihood Determination (Section 5)
- Step 6 - Impact Analysis (Section 6)
- Step 7 - Risk Determination (Section 7)
- Step 8 - Control Recommendations (Section 8)
- Step 9 - Results Documentation (Section 9)

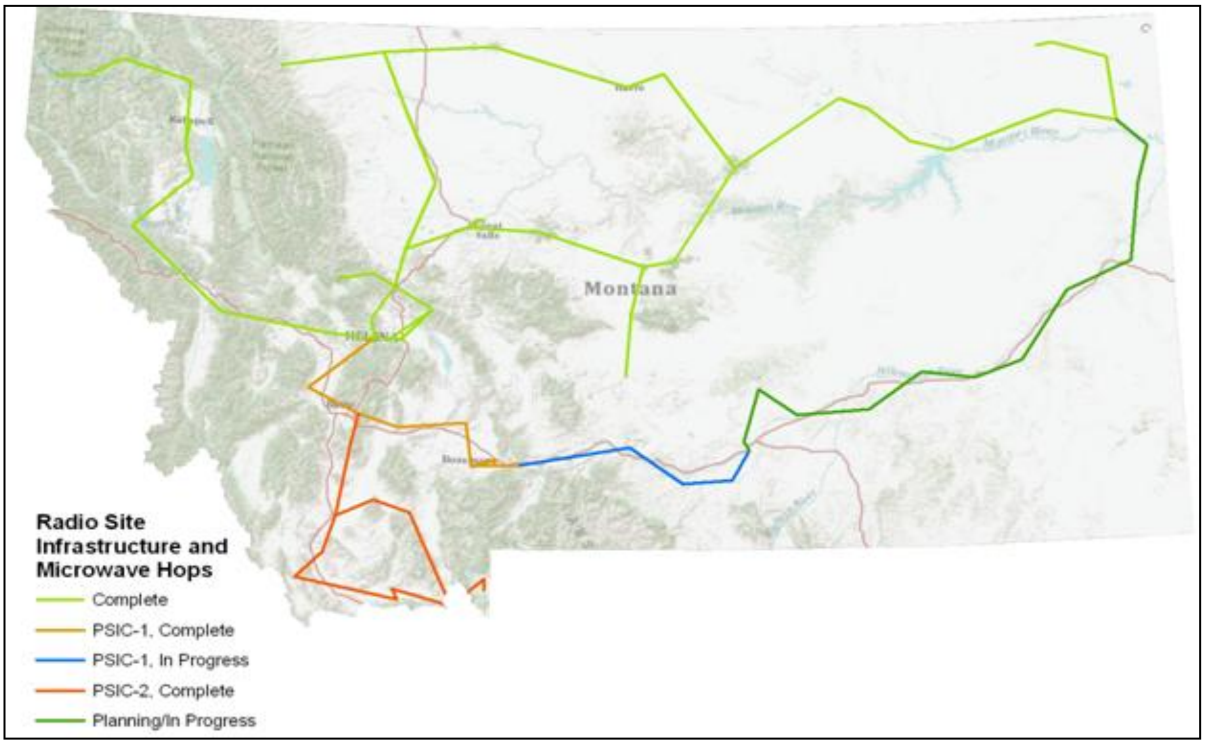
Each section builds upon the information derived from the previous section. This risk assessment pertains to the enterprise alerting and monitoring of the Microwave and Radio system as described in the Strategic Alerting and Monitoring Architecture for the Statewide Microwave Network.

1 SYSTEM CHARACTERIZATION

The Interoperability Montana statewide microwave/radio communications system is used by public safety responders. The wide-area system operates narrowband in the VHF frequency range and uses a protected high-capacity digital microwave backbone for voice and data interconnect traffic.

The digital microwave equipment used throughout the State of Montana is made up of 44 sites and master site controlling connectivity. The diagram below shows the connectivity of the microwave network across the state.

Figure 1a: Microwave Network Path Map



The green lines in Figure 1a represent built out connectivity; blue lines represent build out in progress, and gold lines state for planned build out.

The system as is exists today is not monitored and is managed by physically accessing the equipment at actual communications site. As described in the architecture document, both remote accessibility for management purposes and event notification (alerting) functionality is to be implemented.

Eight management services are part of the microwave network. They are:

1. ProVision
2. Motorola – Unified Network Configurator (UNC)
3. Motorola – Unified Event Manager (UEM)
4. Juniper – Firewall and VPN Manager
5. RSA Manager (2nd factor authentication)
6. Motorola – User Configuration Manager (UCM)
7. Motorola – Zone Controller Manager (ZCM)
8. Microsoft Active Directory (AD)

Each service has three basic functions:

1. Management (including configuration, i.e. moves, adds, and changes)
2. Monitoring
3. Alerting of events

Access and notifications of these systems will be governed by policies defined for groups or types of users. The groups are set up according to job functions. The job function defines what type of access is needed for each service. An individual user gains access to the system based on the group.

As part of the new access controls, four types of groups are defined:

1. Enterprise Administrator
2. Zone Administrator
3. Site Administrator
4. Monitoring Administrator

The following matrix shows the service by group, and what function they are able to perform.

1. Enterprise Administrator

Management System	Monitoring	Alerting	Configuration
1. Provision	Y	Y	Y
2. UNC	Y	Y	Y

3. UEM	Y	Y	Y
4. Juniper FW Manager	Y	Y	Y
5. RSA Manager	Y	Y	Y
6. UCM	Y	Y	Y
7. ZCM	Y	Y	Y
8. Active Directory	Y	Y	Y

2. Zone Administrator

Management System	Monitoring	Alerting	Configuration
1. Provision	Y	N	N
2. UNC	Y	N	N
3. UEM	Y	N	N
4. Juniper FW Manager	Y	N	N
5. RSA Manager	Y	N	N
6. UCM	Y	Y	Y
7. ZCM	Y	Y	Y
8. Active Directory	Y	N	N

3. Site Administrator

Management System	Monitoring	Alerting	Configuration
1. Provision	Y	Y	N
2. UNC	Y	Y	N
3. UEM	y	Y	N
4. Juniper FW Manager	Y	N	N
5. RSA Manager	Y	N	N
6. UCM	Y	Y	Y
7. ZCM	Y	Y	Y
8. Active Directory	Y	N	N

4. Monitoring Administrator

Management System	Monitoring	Alerting	Configuration
1. Provision	Y	Y	N
2. UNC	Y	Y	N
3. UEM	Y	Y	N
4. Juniper FW Manager	Y	Y	N
5. RSA Manager	Y	Y	N
6. UCM	Y	Y	N
7. ZCM	Y	Y	N
8. Active Directory	Y	Y	N

The proposed system performs three security processes using industry standards and procedures. The three processes are:

1. Authentication
2. Authorization
3. Accounting

An individual authenticates to the enterprise system using a two-form factor. Two-factor authentication requires the user's individual password* and a random key generated using an RSA token. The password adheres to the policy for password management as shown in Appendix B. The authorization process ensures the individual is allowed to access the enterprise service. The user is granted access to services as defined by the group they belong to and nothing else. With full accounting, all activity by an individual when accessing or attempting to access enterprise systems is logged and recorded.

2 THREAT IDENTIFICATION

An issue that greatly complicates the prevention of threat actions is that the basic intent of the attack often cannot be determined. Both internal and external threat sources may exist. Internal attacks may be executed by threat actors such as disgruntled employees and contractors. It is important to note that non-malicious use by threat operators may result in system vulnerabilities being exploited. Internal threat operators can on their own or under the direction of an external threat source (for example, an employee may install a screensaver that contains a Trojan horse) internal threat agents currently account for the majority of intentional attacks against government and commercial enterprises.

Transnational threats are generated by organized non-state entities such as drug cartels, crime syndicates, and terrorist organizations. The nature of the transnational external threat makes it more difficult to trace and provide a response.

This section provides a list of threat-sources that could exploit system vulnerabilities according to the four most common threat sources, which are:

1. Natural
2. Human
3. Environmental
4. System Design

Natural Threat Source: The most common natural threat sources in Helena, Montana (where the core radio systems are located) are fires, floods, and earthquakes.

Human Threat Source: These are events that are either enabled by or caused by human beings, such as unintentional acts or deliberate actions.

Environmental Threat Source: These are events such as long-term power failure, pollution, chemical or liquid leakage. If the environmental threat is caused or enabled by human beings, then the threat source is considered human. Environmental threats discussed in this document are considered to have no human motivation.

System Design Threat Source: Failure to implement, operate and manage a system in accordance with the design specifications and established procedures and policies can result in marginalized reliability or service.

Motivation and Threat Actions:

The tables below contain perceived threats to the microwave alerting and monitoring system arrayed by threat type. Table 2a below illustrates Natural Threat Sources. Natural Threat Sources do not typically have a motivation, but are the result of a natural act. The threat Tables 2a-2d below are not intended to be all-inclusive list of threats to the microwave alerting and monitoring system. Any threat that has already had a control mechanism put in place to eliminate or reduce the threat to an acceptable level is not listed. It is also possible that future threats may arise that are currently unknown or indefinable at this time.

Table 2a Natural Threat Matrix

Threat Source		Threat Action
Fire		Services are destroyed
Flood		Services are destroyed
Earthquake		Services are destroyed

Table 2b Human Threat Matrix

Threat Source	Motivation	Threat Action
Hacker	Challenge Ego Rebellion Sabotage	Hacking Social Engineering System Intrusion Break In Unauthorized System Access
Computer Criminal Continued from above	Destruction of information Illegal Information disclosure Monetary Gain Unauthorized Data Alteration	Computer Crime Stalking Fraudulent Act Impersonation Information Bribery Spoofing System Intrusion/Compromise of system Destruction of System
Terrorist	Blackmail Destruction Exploitation Revenge Monetary Gain Sabotage	Bomb/ Terrorism Information Warfare System attack Denial of Service System Penetration System Tampering Destruction of System

Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary Gain Revenge Unintentional Errors & Omissions	Assault on an employee Blackmail Browsing of Proprietary Information Computer abuse Fraud and theft Information Bribery Input of Falsified Corrupted Data Malicious Code Bomb, Trojan Horse Sale of Personal Information System bugs System Intrusion System Sabotage Unauthorized System Unauthorized system access

Table 2c Environmental Threat Matrix

Threat Source		Threat Action
Long-Term Power Failure		Services are unusable
Pollution		Services may be unusable or marginalized
Chemical, or Liquid Leakage		Services are destroyed

Table 2d System Design Threat Table

Threat Source		Threat Action
Lack of established life-cycle process		Equipment may fail at inconvenient times
Lack of fault tolerant elements		Services may be unusable or marginalized when equipment fails
Lack of offsite backup of system data		Services are destroyed
Lack of password policy and validation		User accounts accessing into the system can be compromised.
Ability to add outside connections into the system		System can be accessed from the connections if not properly secured

3 VULNERABILITY IDENTIFICATION

The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by potential threat sources to the system. This section builds upon the previous section's information. The threat source matrix is expanded to individually define perceived vulnerability to the system. A threat action has also been added to each identified vulnerability.

Table 3a Potential Vulnerabilities Matrix

Vulnerability	Threat Source	Threat Action
Insufficient verification of data	Hacker/Cracker/ Computer Criminal/ Terrorist/ Insider Threat	Man-in-the-middle attacks
Low bandwidth	Hacker/Cracker/ Computer Criminal/ Terrorist/ Insider Threat	Service shutdown
Filter/resource manipulation flaws	Implementation team	Insecure access to files
Password Management	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Compromise of username and passwords
Permissions and privileges	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Escalated rights and privileges
Eavesdropping	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Failure to encrypt point-to-point. Compromise effectiveness of the system
Authentication and Certificate errors	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Registration spoofing Valid user registration
Error handling	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Brute force attack on only valid accounts
Homogenous Network	Implementation Team	Network outage
Redundancy failure	Implementation Team	Network outage
Physical connection quality and packet collision	Implementation Team	Packet loss Network latency Jitter
Destruction of System	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat/ Natural Disaster	Threat Actions listed above, and unknown ones
System Sabotage	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Threat Actions listed above, and unknown ones
Compromising of System	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Gathering of information to gain access to the system to marginalize the use of the system

Long-Term Power Failure	Hacker/Cracker/ Computer Criminal/ Terrorist/Insider Threat	Services are unusable
Pollution	Natural Event	Services may be unusable or marginalized
Chemical, or Liquid Leakage	Natural Event	Services are destroyed
Fire	Natural Event	Services are destroyed
Flood	Natural Event	Services are destroyed
Earthquake	Natural Event	Services are destroyed
Lack of established life-cycle process	Lack of Process and Procedure	Services may be unusable or marginalized
Lack of fault tolerant elements	Lack of Planning/Implementation	Services may be unusable or marginalized
Lack of offsite backup of system data	Lack of Process and Procedures	Systems may be unusable or marginalized while systems are rebuilt
Lack of password policy and validation	Lack of Process and Procedures	Human Threats may be easier to carry out
Ability to add outside connections into the system	Lack of Centralized Management	Human Threats may be easier to carry out

Vulnerability Sources:

Information for this document was gleaned from:

1. The National Institute of Building Science Threat/Vulnerability Assessment and Risk Architecture section.
2. National Institute of Standards and Technology (NIST) Computer Security Division.

4 CONTROL ANALYSIS

The goal of this step is to analyze the controls that are planned for implementation to minimize or eliminate the likelihood of a threat exercising system vulnerability. As mentioned previously, if a threat has a control already in place, additional control analysis is not required.

To derive an overall likelihood rating that indicates that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered. For example, vulnerability (e.g., system or procedural weakness) is not likely to be exercised if the likelihood is low.

Control Methods

Security controls encompass the use of technical and non-technical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non-technical controls are management and operational controls such as security policies; operational procedures; and personnel, physical, and environmental security.

Control Categories

The categories for technical and non-technical control methods may be further classified as preventive or detective. These two sub-categories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails and intrusion detection methods.

Control Analysis Technique

The development of a security requirements checklist or use of an available checklist is helpful in analyzing controls in an efficient and systematic manner. A security requirements checklist may be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements).

5 LIKELIHOOD DETERMINATION

Having determined what threats are important and what vulnerabilities exist to be exploited, the likelihood of the vulnerability occurring may be assessed. It is useful to estimate the likelihood of possible risks. In security, "likelihood" is a qualitative estimate of how successful the attack will be. Since analysis is based on past experience, this approach cannot account for new types of attacks or vulnerabilities. Further, this approach may not accurately reflect the *probability* of a successful attack. Nonetheless, the concept of likelihood can be useful when prioritizing risks and evaluating the effectiveness of potential mitigations.

The following factors must be considered in the likelihood estimation:

- the threat's motivation and capability
- the vulnerability's directness and impact
- the effectiveness of current controls

The threat's motivation and capability can vary widely. A college student who hacks for fun is less motivated than a hacker who is compensated or promised a monetary reward. A former employee who has a specific grievance against a company will be more motivated and informed than an outsider who has no special knowledge of the target system's internal workings.

Some vulnerabilities are direct and have severe impacts. For example, vulnerability is very direct and severe if it allows a database server to be compromised directly from the Internet using a widely distributed exploit kit. A less severe, indirect vulnerability may cause an exploit payload to pass unmodified through different systems. This can result in log entries that produce unexpected logging system failures. The effectiveness of current controls characterizes how high the bar is set for an intentional attacker or how unlikely an accidental failure is. For example, simple user ids and passwords may be compromised more easily than two-factor authentication systems. Adding a second authentication factor raises the bar for a would-be threat. However, if the second factor in the authentication is a biometric thumbprint reader that can be spoofed with latent image recovery techniques, the additional controls are not as effective.

The likelihood is a subjective combination of these three qualities (motivation, directness of vulnerability, and compensating controls). These can be boiled down to a rating of high, medium, or low. These rating levels are established by security industry standards. The likelihood matrix for the microwave/radio system uses definitions from Table 5c below:

Table 5a Likelihood Definition Table

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable. Controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable. Controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability. Or, controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

The vulnerabilities defined in the previous section are included in the matrix shown in Table 5b below and include the likelihood of the vulnerability occurring.

Table 5b Potential Vulnerabilities Likelihood Table

Vulnerability	Likelihood Level
Ability to add outside connections into the system	H
Authentication and Certificate errors	H
Chemical, or Liquid Leakage	H
Compromising of System	M
Destruction of System	M
Earthquake	H
Eavesdropping	L
Error handling	H
Filter/resource manipulation flaws	H
Fire	M
Flood	M
Homogenous Network	H
Insufficient verification of data	H
Lack of established Life-cycle process	H
Lack of fault tolerant elements	H
Lack of offsite backup of system data	H
Lack of password policy and validation	H
Long-Term Power Failure	H
Low bandwidth	H
Password Management	H
Permissions and privileges	H
Physical connection quality and packet collision	H
Pollution	L
Redundancy failure	M
System Sabotage	M

6 IMPACT ANALYSIS

Independent of likelihood and controls, the risk's impact must be determined. Impact may be described as the consequences if the system faces the worst-case scenario. Further, analysis must account for other credible scenarios that are not the worst case yet are enough to warrant attention.

To determine the overall impact of vulnerability, three aspects of the risk must be evaluated:

1. Identify Threatened Assets
2. Identify Locality Impact

3. Identify Public Safety Impact (The impact must be related to #1 and #2 above.)

Identify Threatened Assets

Common impacts to information assets include loss of data, corruption of data, unauthorized or unaudited modification of data, unavailability of data, corruption of audit trails, and insertion of invalid data.

The only elements of the system discussed in this assessment are microwave and radio transport. Individual radios are not considered part of the system.

Identify Business Impact

The radio system will suffer a degree of impact if an attack takes place, this degree of impact is referred to as business impact. It is of paramount importance to characterize that impact in as specific terms as possible. As an example, if the worst consequence of a lightning strike occurred at a tower site, the cost to replace the equipment is around $420,000.00. Assume the cost to implement R56 grounding is approximately $16,000.00, the return on investment for mitigation ($16,000.00) needs to be weighed against the impact of losing an entire site ($420,000.000.

Impact Locality

All impacts have a locality in space, time, policy, and law. In addition to characterizing the monetary impact, the location in other dimensions may be useful or required. For example, if an encryption key is stored unencrypted, it matters whether that key is in the dynamically allocated RAM of an application on a trusted server, on the hard disk of a server on the Internet, or in the memory of a client application.

Impacts maybe localized in time or within business and technical boundaries. For example, a failure in the master zone controller located in Helena, Montana results in the administrators not being able to reconfigure radios. If an incident required radio talk groups to interoperate, reconfiguring on the fly would not be possible if the zone controller was unavailable.

The impact locality is assumed to be the inability of an individual or group of radios from sending or receiving transmissions.

Once individual areas of the impact are evaluated, the overall impact may be determined. Again, the overall rating is boiled down to high, medium, or low. These rating levels are established industry standards in the security field. The impact matrix for the microwave/radio system will use the definitions as defined in Table 6a below:

Table 6a Magnitude of Impact Definitions Table

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; or (2) may noticeably affect an organization's mission, reputation, or interest.

Table 6b below shows each vulnerability (as defined in the previous section) and the associated overall impact and magnitude of the impact.

Table 6b Magnitude of Impact Table

Vulnerability	Overall Impact	Magnitude Of Impact
Insufficient verification of data	Elements of the system could modified or deleted	High
Low bandwidth	Services would be unavailable or switch into local mode	High
Filter/resource manipulation flaws	Elements of the system could modified or deleted	High
Password Management	Systems would continue to function; elements could not be added or modified	Medium
Permissions and privileges	Escalated rights and privileges result in modifying, adding, or removing elements	Low
Eavesdropping	Failure to encrypt point-to-point resulting in capturing of read/write strings, passwords or sensitive data such as listening to a conversation	Low

Authentication and Certificate errors	Elements of the system could modified or deleted	High
Error handling	Elements of the system could modified or deleted	High
Homogenous Network	Network outage resulting in system being unavailable	High
Redundancy failure	Network Outage resulting in system being unavailable	High
Physical connection quality and packet collision	Services may be marginalized	Low
Destruction of System	Services are destroyed	High
System Sabotage	Services are marginalized or destroyed	High
Compromising of System	Effectiveness of services may be marginalized i.e. Listening in on law enforcement conversations or spoofing of new speakers	Medium
Long Term Power Failure	Services are unusable unless backup power is functional	High
Pollution	Services may be unusable or marginalized	Low
Chemical, or Liquid Leakage	Services are destroyed	High
Fire	Services are destroyed	High
Flood	Services are destroyed	High
Earthquake	Services are destroyed	High
Lack of established life-cycle process	Services may be unusable or marginalized	High
Lack of fault tolerant elements	Services may be unusable or marginalized	High
Lack of offsite backup of system data	Systems may be unusable or marginalized while systems are rebuilt	High
Lack of password policy and validation/audit	Human threats may be easier to carry out	High
Ability to add outside connections to the system	Human Threats may be easier to carry out	High

7 RISK DETERMINATION

Risk determination combines the likelihood of a risk occurring with the impact of the risk. The product of these two sets of analysis provides an overall summary of risk exposure. The risk determination generalizes the overall exposure of the system relative to a given risk and offers more detailed visibility of both impact and likelihood. The risk determination gives the Interoperability Montana more fine grained control over risk management, but does not require all risks to be eliminated.

Risk Level Matrix:

The matrix displayed in Table 7a shows how the overall risk levels of High, Medium, and Low are derived. The rationale for this justification is explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low. The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low. These levels are established industry standards in the security field. The risk level matrix for the microwave/radio system will use the definitions as defined in Table 7a below:

Table 7a Risk-Level Matrix

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Table 7b combines information from Tables 5b, Potential Vulnerabilities Likelihood; and 6b, Magnitude of Impact. Each vulnerability listed below multiplies the value associated with threat likelihood with the impact. The product is a risk level score. Table 7b is displayed below:

Table 7b Risk Level Table for Defined Vulnerabilities

Vulnerability	Threat Likelihood	Impact	Score
Ability to add outside connections into the system	High (1.0)	High (100)	100
Authentication and Certificate errors	Low (0.1)	High (100)	10
Chemical, or Liquid Leakage	Low (0.1)	High (100)	10
Compromising of System	Medium (0.5)	Medium (50)	25
Destruction of System	Medium (0.5)	High (100)	50
Earthquake	High (1.0)	High (100)	100
Eavesdropping	Low (0.1)	Low (10)	1
Error handling	Low (0.1)	High (100)	10
Filter/resource manipulation flaws	Low (0.1)	High (100)	10
Fire	Medium (0.5)	High (100)	50
Flood	Medium (0.5)	High (100)	50
Homogenous Network	High (1.0)	High (100)	100

Insufficient verification of data	Low (0.1)	High (100)	10
Lack of established Life-cycle process	High (1.0)	High (100)	100
Lack of fault tolerant elements	High (1.0)	High (100)	100
Lack of offsite backup of system data	High (1.0)	High (100)	100
Lack of password policy and validation/ audit	High (1.0)	High (100)	100
Long Term Power Failure	Low (0.1)	High (100)	10
Low bandwidth	Low (0.1)	High (100)	10
Password Management	Low (0.1)	Medium (50)	5
Permissions and privileges	Low (0.1)	Low (10)	1
Physical connection quality and packet collision	High (1.0)	Low (10)	10
Pollution	Low (0.1)	Low (10)	10
Redundancy failure	High (1.0)	High (100)	100
System Sabotage	Medium (0.5)	High (100)	50

As explained earlier in this document, all system access is challenged using two-form factor authentication. The second form of authentication is accomplished using the RSA security system from EMC Corp. With the implementation of RSA technology, the likelihood of vulnerabilities exploiting authentication or authorization is low and is reflected with the low values for those vulnerabilities as shown in the table above.

Risk Scale

The industry accepted Risk Scale is as follows:

- High >51 to 100
- Medium >11 to 50
- Low 1 to 10

Vulnerabilities that have a calculated risk of "low" do not have a control recommendation; however, these noted vulnerabilities remain in the risk assessment and will be re-evaluated in the next update of this document. The vulnerabilities with a low risk level are provided below. Please note that the numbered list does not represent priority:

1. Authentication and Certificate Errors
2. Chemical, or Liquid Leakage
3. Eavesdropping
4. Error Handling
5. Filter/Resource Manipulation flaws
6. Insufficient verification of data
7. Long-Term Power Failure
8. Low Bandwidth

9. Password Management
10. Permissions and Privileges
11. Physical connection quality and packet collision
12. Pollution

Vulnerabilities showing a risk of “medium” or “high” are included in the control recommendation portion of this document. Vulnerabilities at medium and high risk are presented below:

1. Ability to add outside connections into the system
2. Compromising of System
3. Destruction of System
4. Earthquake
5. Fire
6. Flood
7. Homogenous Network
8. Lack of established Life-cycle process
9. Lack of fault tolerant elements
10. Lack of offsite backup of system data
11. Lack of password policy and validation/ audit
12. Redundancy Failure
13. System Sabotage

8 CONTROL RECOMMENDATIONS

Control Methods

Control methods used in this document are divided into five categories:

1. Avoidance
2. Loss Prevention
3. Loss Reduction
4. Segregate Loss
5. Contractual Loss

Here is a description of control categories:

- **Avoidance** – Risk is high; one would not want to assume the risk and it can’t be transferred to avoid the risk altogether. This method eliminates any possibility of loss. It is achieved either by abandoning or never undertaking an activity or asset.

- **Loss Prevention** – Reduces the frequency or likelihood of a “particular” loss. Examples include:
    - Improved security measures to reduce the possibility of arson or theft.
    - Improved maintenance of facilities to reduce the possibility of a tripping hazard.
- **Loss Reduction** – Reduces the severity or cost of a “particular” loss. Here are some examples:
    - Require the use of seatbelts to reduce the chance of bodily injury in a vehicle collision.
    - Require the use of hearing protection to reduce the chance of a hearing loss.
- **Contractually Transfer the Risk** - Places the financial responsibility for a risk to a third party or the person/entity closest to and best able to control the activity and/or its outcome.
- **Segregate Losses** – Arrange the system to prevent one event from causing loss to the whole via one or both of these methods: duplication and separation.
    - **Separation** – Activities or assets are distributed among multiple locations.
    - **Duplication** –Spare or duplicates are relied on but are only used if assets or activities suffer a loss.

The goal of various recommended controls is to reduce the level of risk to both the system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendation table (Table 8a) below applies to any vulnerability with a medium or high risk:

Table 8a Control Recommendation Table

Vulnerability	Control Method	Control Category Control Sub Category	Control Recommendation
Homogenous Network	Technical	Loss Prevention Preventive Detective	Establish procedures for implementation and operations. Perform validation of work
Redundancy Failure	Technical	Loss Prevention Preventive Detective	Establish procedures for implementation and operations. Perform validation of work

Compromising of System	Technical	Loss Prevention Preventive Detective	Establish procedures for allow access into the system. Monitor system.
Fire	Non-Technical Operational	Loss Reduction Preventive	Ensure adequate fire suppression is in place. Follow business continuity plan if system is destroyed.
Flood	Non-Technical Operational	Loss Reduction Preventive	Ensure adequate flood protection is in place. Follow business continuity plan if system is destroyed
Earthquake	Non-Technical Operational	Loss Reduction Preventive	Ensure building is adequate to survive an earthquake. Follow business continuity plan if system is destroyed
Lack of established life-cycle processes	Non-Technical Management	Loss Reduction Preventive Detective	Establish procedures for life-cycle management. Perform validation of work
Lack of fault tolerant elements	Non-Technical Management	Loss Reduction Preventive	Define strategic architecture
Lack of off-site storage of data	Non-Technical Management	Segregate Loss Preventive Detective	Establish procedures for business continuity. Perform validation of work
Lack of password policy and validation/audit	Non-Technical Management	Loss Prevention Preventive Detective	Establish procedures for password management. Perform validation of work
Ability to add/audit outside connections to system	Non-Technical Management	Loss Prevention Preventive Detective	Establish enterprise method of outside connections. Perform validation of work

9 RESULTS & RECOMMENDATIONS

The control recommendations listed above are the results of the risk assessment process. It is during the risk assessment process that procedural and technical security controls are evaluated, prioritized, and implemented. It should be noted that not all possible recommended controls may be implemented to reduce loss. A cost-benefit analysis should be conducted to demonstrate that the costs of implementing controls can be justified by a reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing recommended options should be evaluated carefully during the risk mitigation process.

The risk assessment process is usually repeated at least every three (3) years for federal agencies, as mandated by the Federal Office of Management and Budget (OMB) Circular A-130. However, risk management should be conducted and integrated in the System Development Life Cycle (SDLC). Since federal financial participation accounts for about 70% of IM funding, a three-year review cycle for risk assessment is warranted.

APPENDIX A: INDEX OF FIGURES AND TABLES

APPENDIX B: PASSWORD POLICY

INTRODUCTION

All employees and personnel that have access to the statewide microwave network must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

1. Purpose

This policy is designed to protect the organizational resources on the statewide microwave network by requiring strong passwords along with protection of these passwords and the establishment of a minimum time between changes to passwords.

2. Scope

The scope of this policy includes all personnel who have or are responsible for any form of access to the statewide microwave network. This policy also applies to all personnel who have any form of account requiring a password on the network including but not limited to a domain account and e-mail account.

3. User-IDs

1. All users, or processes acting as users, must be positively identified to the network with a unique User-ID that is assigned by the Enterprise Radio System Administrator.
2. Employees and other authorized users shall not share User-IDs.
3. Employees and other authorized users shall not reuse User-IDs.
4. A User-ID shall have access removed when the individual user no longer needs access to the network, or be deactivated when the individual user no longer needs access to the network or terminates employment. Managers must notify Radio System Administrator within 24 hours of the termination of an employee so that the User-ID may be deactivated. Notification by the manager is preferred at least three days before the user terminates.
5. User-IDs shall be deactivated by the Radio System Administrator if unused for more than 90 days.

4. Passwords

1. All User-IDs that are not restricted must have a password or a stronger mechanism associated with them to ensure that only the authorized user is able to utilize the User-ID.
2. Passwords must be at least eight characters long. More complex passwords containing uppercase, lowercase, and numeric characters are recommended.
3. Passwords shall be changed at least every 60 days and cannot be reused for at least six cycles.
4. The warning level to users for forced password changes must be seven days or greater for systems that support this capability.
5. Passwords are not to be written down, inserted into email messages or other forms of electronic communication, and are not to be shared with other individuals. If passwords must be kept in a place to be viewed, they must be kept in an encrypted password vault.
6. Passwords are not to be easily guessed words or other information such as the user's name, address, phone number, spouse's name, a child's name, pet's name, etc.
7. The password cannot be the same as the User-ID, including the initial password.
8. Initial passwords assigned to a new User-ID must be changed by the user at their initial login. Passwords that have been reset by the Radio System Administrator are also to be changed by the user as soon as they log into the system.
9. All vendor-supplied default passwords must be changed by the Radio System Administrator before any network or software is used in production.
10. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.
11. After six attempts of providing the correct password for an account, the account shall be locked for a period of at least eight hours.

5. Remote Access

Remote access must use multifactor authentication.

6. Device Authentication

1. All internal networks must be configured such that they can prevent and/or detect attempts to connect from unauthorized devices.

2. All devices gaining access to the statewide microwave network shall be authenticated to a device management system.

7. General Identification and Authentication Requirements

1. Developers are prohibited from building or deploying secret User-IDs or passwords which have special privileges and which are not clearly covered in the system documentation.
2. The use of local individual user accounts on a device or system by employees or other authorized users is prohibited.
3. Authentication systems shall not display authentication information (passwords) during the authentication process.
4. An Information System user may have not more than one concurrent session for an Information System.
5. An Information System shall initiate a session lock after 15 minutes of inactivity for both local and remote sessions that connect to the Information Systems "console". Application-only sessions are exempt from this requirement.

8. System Generated Passwords

Authorized users shall not store system-generated passwords for service accounts and storage of these must not be stored in readable format i.e. batch files, scripts, etc.

9. Compliance

Compliance shall be evidenced by implementation of the identification and authentication requirements as described above.

10. Enforcement

Since password security is critical to the security of the statewide microwave network, users who do not adhere to this policy may be subject to disciplinary action.